## CLAIMS

What is claimed is:

1. An automation security system, comprising:

an asset component to define one or more factory assets;

an access component to define one or more security attributes associated with the factory assets; and

a security component to regulate access to the factory assets based upon the one or more security attributes.

2. The system of claim 1, the one or more or more security attributes including at least one of a role attribute, a time attribute, a location attribute, and an access type attribute.

3. The system of claim 1, the security component is based on at least one of a formal threat analysis, a vulnerability analysis, a factory topology mapping and an attack tree analysis.

4. The system of claim 3, the security component is based on at least one of automation and process control security, cryptography, and Authentication/ Authorization/Accounting (AAA).

5. The system of claim 1, the asset component describes at least one of factory components and groupings, the factory components are at least one of sensors, actuators, controllers, I/O modules, communications modules, and human-machine interface (HMI) devices.

6. The system of claim 5, the groupings include factory components that are grouped into at least one of machines, machines grouped into lines, and lines grouped into facilities.

7. The system of claim 5, the groupings have associated severity attributes such as at least one of risk and security incident cost.

8. The system of claim 7, further comprising an ISA S95 Model for Enterprise to Control System Integration to integrate security aspects across or within respective groupings.

9. The system of claim 1, further comprising a set of generic IT components and specifies parameters to assemble and configure the IT components to achieve flexible access to the one or more factory assets.

10. The system of claim 9, the IT components include at least one of switches with virtual local area network (VLAN) capability, routers with access list capability, firewalls, virtual private network (VPN) termination devices, intrusion detection systems, AAA servers, configuration tools, and monitoring tools.

11. The system of claim 1, further comprising security parameters and policies that are developed for physical and electronic security for various component types.

12. The system of claim 11, the security parameters and policies further comprising at least one of security protection levels, identification entry capabilities, integrity algorithms, and privacy algorithms.

13. The system of claim 1, the security component includes at least one of authentication software, virus detection, intrusion detection, authorization software, attack detection, protocol checker, and encryption software.

14. The system of claim 13, the security component at least one of acts as an intermediary between an access system and one or more automation components, and facilitates communications between the access system and the one or more automation components.

15. The system of claim 2, the security attributes are specified as part of a network request to gain access to the one or more factory assets, the security attributes included in at least one of a group, set, subset, and class.

16. The system of claim 15, the security component employs at least one authentication procedure and an authorization procedure to process the network request.

17. The system of claim 16, further comprising one or more security protocols including at least one of Internet Protocol Security (IPSec), Kerberos, Diffie-Hellman exchange, Internet Key Exchange (IKE), digital certificate, pre-shared key, and encrypted password, to process the network request.

18. The system of claim 15, further comprising at least one of an access key and a security switch to control network access to a device or network.

19. The system of claim 18, the access key further comprises at least one of time, location, batch, process, program, calendar, GPS (Global Positioning Information) to specify local and wireless network locations, to control access to the device or network.

20. An automation security system, comprising:

one or more servers that manage a network interface between networked factory assets and other devices or users attempting access to the networked factory assets; and

a security management module associated with the network interface for enforcing an enterprise wide policy and to manage security threats directed to the networked factory assets.

21. The system of claim 20, the security management module at least one of schedules audits, establishes a security policy, applies the policy from a single or distributed console, and generates reports that identify potential weaknesses in security.

22. The system of claim 20, the security management module provides an interface to at least one of add, delete and modify security rights of an individual, a group, or a device and distribute security information to various controllers and control devices.

23. The system of claim 20, further comprising at least one of:

an authentication with the one or more servers to establish a secure link;

a secure link to authenticate and authorize access to a requestor of the networked factory assets; and

establishment of a secure session with the requestor if access is authorized.

24. An automation security methodology, comprising:

analyzing one or more automation assets;

modeling the automation assets in accordance with network security considerations; and

developing a security framework for an automation system based in part on the modeling of the automation assets and a network access type.

25. The method of claim 24, further comprising analyzing one or more security attributes to determine whether access should be granted to the one or more automation assets.

26. The method of claim 25, the one or more security attributes further comprise at least one of a role, an asset type, a location, a time, and an access type.

27. The method of claim 24, further comprising at least one of:

determining whether to grant access to the one or more automation assets;

granting access from the one or more automation assets; and

granting access from a network device associated with the one or more automation assets.

28. An automated security system for an industrial control environment, comprising:

means for defining one or more security attributes associated with at least one network request;

means for processing the one or more security attributes; and

means for controlling access to at least one of a network device and an automation component based in part on the one or more security attributes.

29. A security schema for a factory automation system, comprising:

a first data field to describe factory assets;

a second data field to describe security parameters for the factory assets; and

a schema to associate the first and second data fields, the schema employed to limit access to the factory assets based upon the security parameters.

30. The system of claim 29, the schema including at least one of an access role, an asset type, an access type, time information, address information, and location information.

31. The system of claim 29, further comprising a response schema to provide status to a requesting network device.

32. The system of claim 31, the response schema including at least one of a status field, a time field, an access type field, an access location field, and a key field.

33. The system of claim 31, the response schema including an attachment field to indicate other security data follows the response schema.